

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-294120

(43)Date of publication of application : 11.11.1997

(51)Int.Cl.

H04L 9/08  
G09C 1/00  
H04L 9/14

(21)Application number : 08-107501

(71)Applicant : HITACHI LTD

(22)Date of filing : 26.04.1996

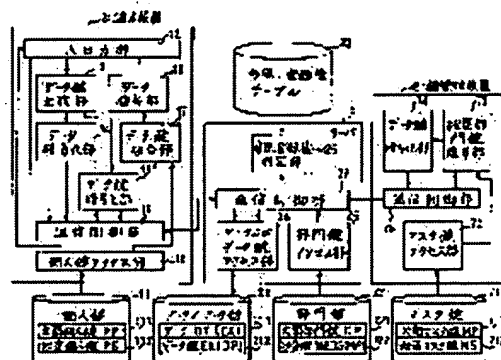
(72)Inventor : SATO MAKOTO  
NANBA AKIRA  
DOMYO SEIICHI  
TAKARAGI KAZUO  
SHIBAHARA SETSUO

## (54) ACCESS CONTROL METHOD AND SYSTEM FOR CIPHERED SHARED DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To allow user groups to share data with security by using a ciphering communication technology.

SOLUTION: A data ciphering section 14 and a data key ciphering section 15 of a terminal equipment 3 cipher data respectively by using a data key generated by a data key generating section 13 and use a public key 221 corresponding to a designated secrecy group to cipher the data key and a server 5 stores the data 211 and a data key 212. In the case of referencing the data 211, the terminal equipment 3 sends the acquired data key 212 and an open individual key 111 to the server 5, the server 5 uses a secret key to decode the data key 212 and uses the open individual key 111 to cipher the decoded data key and sends the result to the terminal equipment 3. A data key decoding section 17 uses a secret individual key 112 to decode the acquired data key and a data decoding section 18 decodes the data.



## LEGAL STATUS

[Date of request for examination]

18.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-294120

(43) 公開日 平成9年(1997)11月11日

(51) Int.Cl. <sup>6</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 B
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B
		7259-5 J		6 3 0 E
H 0 4 L 9/14			H 0 4 L 9/00	6 0 1 E
				6 4 1

審査請求 未請求 請求項の数5 O L (全 9 頁)

(21) 出願番号 特願平8-107501

(22) 出願日 平成8年(1996)4月26日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 佐藤 真

東京都江東区新砂一丁目6番27号 株式会社日立製作所公共情報事業部内

(72) 発明者 難波 電

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 道明 誠一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 高橋 明夫

最終頁に続く

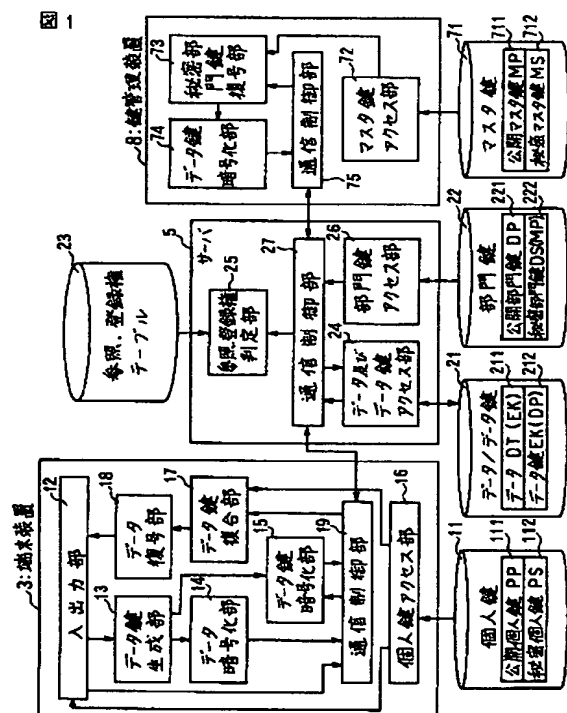
(54) 【発明の名称】 暗号化された共有データのアクセス制御方法及びシステム

(57) 【要約】

【課題】 暗号化通信技術を用いてユーザグループの間で安全にデータを共有する。

【解決手段】 端末装置3のデータ暗号化部14及びデータ鍵暗号化部15は、それぞれデータ鍵生成部13が生成したデータ鍵によってデータを暗号化し、指定された機密区分に対応する公開部門鍵221を用いてデータ鍵を暗号化し、サーバ5にデータ211及びデータ鍵212を格納する。データ211を参照するとき、端末装置3は取得したデータ鍵212及び公開個人鍵111をサーバ5へ送信し、サーバ5は鍵管理装置8を介して秘密マスク鍵712によって秘密部門鍵222、秘密部門鍵によってデータ鍵212を復号し、公開個人鍵111を用いて復号されたデータ鍵を暗号化して端末装置3へ送信する。データ鍵復号部17は秘密個人鍵112を用いて取得したデータ鍵を復号し、データ復号部18がデータを復号する。

図1



## 【特許請求の範囲】

【請求項 1】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるシステムのアクセス制御方法であって、

端末装置によってデータ鍵を生成し、該データ鍵を用いてデータを暗号化し、指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信し、

該サーバによって該データと該データ鍵とを共有データとして記憶装置に格納し、

端末装置によって該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サーバへ送信し、

該サーバによって該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該端末装置へ送信し、

該端末装置によって秘密個人鍵を用いて該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号することを特徴とする暗号化された共有データのアクセス制御方法。

【請求項 2】該端末装置によって該データと該データ鍵とを取得する前に、該サーバによってユーザが属するユーザグループと該ユーザグループに許可されるデータ参照の機密区分とから該データを参照する権限の有無を判定することを特徴とする請求項 1 記載の暗号化された共有データのアクセス制御方法。

【請求項 3】さらに該端末装置によって該サーバから該データ鍵を取得し、受け取った該データ鍵と変更後の機密区分とを該サーバへ送信し、

該サーバによって該秘密部門鍵を用いて受け取った該データ鍵を復号し、指定された機密区分に対応する公開部門鍵によって復号したデータ鍵を暗号化し、該記憶装置に格納される元の該データ鍵を変更後の暗号化したデータ鍵によって更新することを特徴とする請求項 1 記載の暗号化された共有データのアクセス制御方法。

【請求項 4】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるシステムのアクセス制御方法であって、

端末装置によってデータ鍵を生成し、該データ鍵を用いてデータを暗号化し指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信し、

該サーバによって該データと該データ鍵とを共有データとして記憶装置に格納し、

端末装置によって該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サ

ーバへ送信し、

該サーバに接続される鍵管理装置によって該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該サーバを経由して該端末装置へ送信し、

該端末装置によって秘密個人鍵を用いて該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号することを特徴とする暗号化された共有データのアクセス制御方法。

10 【請求項 5】公開個人鍵と対応する秘密個人鍵とを保持する複数の端末装置と、機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持するサーバとがネットワークによって接続されるアクセス制御システムであって、

該端末装置は、データ鍵を生成し、該データ鍵を用いてデータを暗号化し指定された機密区分に対応する公開部門鍵を用いて該データ鍵を暗号化し、暗号化されたデータとデータ鍵とを該サーバへ送信する手段と、該サーバから該データと該データ鍵とを取得し、公開個人鍵と受け取った該データ鍵とを該サーバへ送信する手段とを有し、

該サーバは、該データと該データ鍵とを共有データとして記憶装置に格納する手段と、該秘密部門鍵を用いて該データ鍵を復号し、該公開個人鍵を用いて復号したデータ鍵を暗号化して該端末装置へ送信する手段とを有し、該端末装置は、さらに秘密個人鍵を用いて受信した該データ鍵を復号し、復号したデータ鍵によって取得した該データを復号する手段を有することを特徴とする暗号化された共有データのアクセス制御システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、暗号化されたデータのアクセス制御方法に係わり、特に暗号化されたデータを同一のアクセス権をもったユーザの間で共有するときのアクセス制御方法に関する。

## 【0002】

【従来の技術】端末装置とサーバ装置との間で暗号通信する方法として、例えば特開平 3 - 2 4 3 0 3 5 号公報は、共通鍵暗号方式に従ってデータをデータ鍵によって暗号化し、データ鍵を公開鍵暗号方式の公開鍵によって暗号化して送信する暗号通信システムを開示する。データの暗号化と復号には同一のデータ鍵を用いるためにデータの暗号化と復号処理が高速に行われる。

【0003】図 8 は、上記暗号通信システムの構成を示す図である。各端末装置 9 0 は、ユーザの数だけの公開個人鍵 P P 1, P P 2, . . . と端末ごとの秘密鍵 T S 1, T S 2, . . . を保持する。サーバ 9 1 は、端末対応の公開鍵 T P 1, T P 2, . . . とユーザの数だけの秘密個人鍵 P S 1, P S 2, . . . を保持する。鍵管理装置 9 2 は、公開マスタ鍵 M P 及び秘密マスタ鍵 M S を

保持する。秘密個人鍵は、公開マスタ鍵MPによって暗号化されている。図中で記号X (Y) は、対象Xが鍵Yによって暗号化されていることを示す。対象Xはデータ、データ鍵、秘密個人鍵などである。端末装置90からサーバ91を利用するユーザ1に対して暗号通信するときには、端末装置90で発生させたデータ鍵EKをユーザ1の公開個人鍵PP1によって暗号化してEK (PP1) となったデータ鍵をサーバ91へ送信する。サーバ91にはユーザ1だけがアクセス権を有する領域に秘密個人鍵PS1 (MP) が保持されているので、ユーザ1はこの秘密個人鍵PS1 (MP) にアクセスし、サーバ91及び鍵管理装置92がPS1 (MP) を復号した後の秘密個人鍵PS1を用いてデータ鍵EK (PP1) を復号し、得られたデータ鍵EKによって端末装置90からサーバ91へ送られたデータDT (EK) を復号することができる。サーバ91から端末装置90に暗号通信するときには、サーバ91で発生させたデータ鍵EKを端末の公開鍵TP1によって暗号化してEK (TP1) となったデータ鍵を端末装置90へ送信する。端末装置90では秘密鍵TS1を用いてデータ鍵EK (TP1) を復号し、得られたデータ鍵EKによってサーバ91から端末装置90へ送られたデータDT (EK) を復号することができる。鍵管理装置92は外部から読み出すことができない公開マスタ鍵MPによって秘密個人鍵PSを暗号化し、秘密マスタ鍵MSによって秘密個人鍵PS (MP) を復号する。

#### 【0004】

【発明が解決しようとする課題】上記従来技術は、暗号通信技術を使って安全にデータの登録と参照を可能とするが、暗号通信は個人対個人の通信に限られており、同一のデータ参照権を有するユーザグループの間でデータを共有するという考え方は見当らない。一方機密性が求められるデータを共有する技術として、強制アクセス制御と呼ばれる技術が知られているが、この技術は特別なオペレーティングシステムによる制御が必要とされ、特定の計算機ハードウェア及びオペレーティングシステムの下でなければ利用できなかった。特別なハードウェアやオペレーティングシステムを導入することなく、安全性の高い暗号通信技術を利用して機密性のあるデータをユーザグループの間で共有する技術が望まれている。

【0005】本発明の目的は、暗号化されたデータをユーザグループの間で安全に共有するアクセス制御方法を提供することにある。

#### 【0006】

【課題を解決するための手段】本発明は、複数の端末装置とサーバ装置とがネットワークによって接続されるシステムのアクセス制御方法であって、端末装置側に公開個人鍵と対応する秘密個人鍵とを保持し、サーバ側に機密区分の各レベルに対応して公開部門鍵とそれぞれ対応する秘密部門鍵とを保持する。端末装置では共通鍵暗号

方式に従ってデータを暗号化し、指定された機密区分に対応する公開部門鍵を用いてデータ鍵を暗号化して、暗号化されたデータとデータ鍵とをサーバへ送信し、サーバによって記憶装置に格納する。サーバに格納された共有データをアクセスするときには、端末装置によってサーバからデータとデータ鍵とを取得し、公開個人鍵と受け取ったデータ鍵とをサーバへ送信し、サーバによって秘密部門鍵を用いてデータ鍵を復号し、公開個人鍵を用いて復号したデータ鍵を暗号化して端末装置へ送信し、端末装置によって秘密個人鍵を用いてデータ鍵を復号し、復号したデータ鍵によって取得したデータを復号する。

#### 【0007】

【発明の実施の形態】以下、本発明のアクセス制御システムの一実施形態について図面を用いて説明する。

【0008】図1は、本実施形態のシステムの構成図である。端末装置3はデータを入力及び出力する装置である。サーバ5は入力されたデータ及びデータ鍵を格納するとともに、データの機密区分に従って部門鍵（ドメインの鍵）を格納する装置である。鍵管理装置8は、部門鍵を復号するためのマスタ鍵を格納し、秘密マスタ鍵によって部門鍵を復号する装置である。本実施形態では、データの暗号化／復号にはともに同一の鍵を用いる共通鍵暗号方式を適用する。またデータを暗号化するときの鍵であるデータ鍵の暗号化／復号にはそれぞれ異なる鍵を用いる公開鍵暗号方式を適用する。

【0009】端末装置3に接続される記憶装置11は、個人鍵として公開個人鍵111と秘密個人鍵112とを格納する。入出力部12は図示しないキーボード／表示装置／記憶装置のような入出力装置からのデータの入出力を制御する制御部である。データ鍵生成部13は、共通鍵暗号方式に従ってデータ鍵を生成する処理部である。データ暗号化部14は、共通鍵暗号方式に従って入力されたデータを生成されたデータ鍵によって暗号化する処理部である。データ鍵暗号化部15は、公開鍵暗号方式に従って生成されたデータ鍵を公開部門鍵221によって暗号化する処理部である。個人鍵アクセス部16は、記憶装置11の個人鍵へのアクセスを制御する制御部である。データ鍵復号部17は、公開鍵暗号方式に従ってサーバ5から受け取ったデータ鍵を秘密個人鍵112によって復号する処理部である。データ復号部18は、共通鍵暗号方式に従って復号されたデータ鍵によってデータを復号する処理部である。通信制御部19は、ネットワークを介して端末装置3とサーバ5との間に公開部門鍵221、データ211、データ鍵212及び公開個人鍵111を送受信するよう制御する制御部である。なお端末装置3にはこの他に個人鍵を生成する処理部が存在する。

【0010】サーバ5に接続される記憶装置21は、データ211及びデータ鍵212を格納する。データ21

1は共通鍵暗号方式に従ってデータ鍵EKによって暗号化された状態で格納され、データ鍵212は公開鍵暗号方式に従って公開部門鍵221によって暗号化された状態で格納される。また記憶装置22は、部門鍵として公開部門鍵221及び秘密部門鍵222を格納する。秘密部門鍵222は公開鍵暗号方式に従って公開マスタ鍵711で暗号化された状態で格納される。参照・登録権テーブル23は、各ユーザのグループについてデータ参照時及びデータ登録時の機密区分のレベルを登録するものであり、サーバ5に接続される記憶装置上に格納される。データ及びデータ鍵アクセス部24は、記憶装置21上のデータ211及びデータ鍵212へのアクセスを制御する制御部である。部門鍵アクセス部26は、記憶装置22上の部門鍵へのアクセスを制御する制御部である。参照・登録権判定部25は、参照・登録権テーブル23を参照して各ユーザが要求するデータ参照及び登録が妥当か否かを判定する処理部である。通信制御部27は、ネットワークを介して端末装置3との間の通信を制御するほかに、ネットワークを介して鍵管理装置8との間に公開個人鍵111、データ鍵及び秘密部門鍵222を送受信するよう制御する制御部である。なおサーバ5には端末装置3を利用するユーザに通常のサービスを提供するモードと、通常のサービスを停止してサーバ5の記憶装置22上の部門鍵を更新するメンテナンスモードとの2つのモードがある。サーバ5がメンテナンスモードのときには、図示しない部門鍵を更新する処理部が動作し、図示しない入出力部から入力されるデータに従って部門鍵を更新する。

【0011】鍵管理装置8に接続される記憶装置71は、マスタ鍵として公開マスタ鍵711及び秘密マスタ鍵712を格納する。マスタ鍵アクセス部72は、記憶装置71上のマスタ鍵へのアクセスを制御する制御部である。秘密部門鍵復号部73は、公開鍵暗号方式に従って秘密マスタ鍵712により秘密部門鍵222を復号し、復号された秘密部門鍵によってデータ鍵212を復号する処理部である。データ鍵暗号化部74は、復号されたデータ鍵を公開個人鍵111によって暗号化する処理部である。通信制御部75は、ネットワークを介して通信制御部27との間の通信を制御する制御部である。なお鍵管理装置8には通常のサービスを提供するモードと、記憶装置71上のマスタ鍵を更新するメンテナンスモードとの2つのモードがあるが、サーバ5と鍵管理装置8とは同時には同じモードでなければならない。鍵管理装置8がメンテナンスモードのときには、図示しないマスタ鍵を更新する処理部が動作し、鍵管理装置8内の図示しない入出力部から入力されるデータに従ってマスタ鍵を更新する。

【0012】端末装置3、サーバ5及び鍵管理装置8は、例えばパソコンのような情報処理装置であり、各制御部及び処理部はハードウェアによって又はこの情報処

理装置の記憶装置に格納するプログラムを実行することによって実現される。

【0013】図2は、データをデータ鍵によって暗号化し、暗号化されたデータとデータ鍵を記憶装置21に格納するまでの端末装置3及びサーバ5の処理の流れを示すフローチャートである。端末装置3の入出力部12は、例えばファイルのようにまとめたデータとその機密区分を入力する(ステップ31)。データ鍵生成部13は、データ鍵EKを生成する(ステップ32)。データ鍵は乱数、日付等を種データとしてこれから生成される。次にデータ暗号化部14は入力されたデータを生成されたデータ鍵によって暗号化する(ステップ33)。次にデータ鍵暗号化部15は、通信制御部19を介してサーバ5へ公開部門鍵の送信要求を送信する(ステップ34)。この送信要求は機密区分の指定を含んでいる。サーバ5の通信制御部27は、この要求を受信し(ステップ51)、ユーザの認証をした後、参照・登録権判定部25は参照・登録権テーブル23を参照して要求されたデータの登録が妥当か否かを判定する(ステップ52)。要求が妥当であれば、部門鍵アクセス部26を介して指定された機密区分に対応する公開部門鍵221を取り出して端末装置3へ送信する(ステップ53)。データ鍵暗号化部15は、通信制御部19を介してこの公開部門鍵221を受信し(ステップ35)、データ鍵EKをこの公開部門鍵221によって暗号化する(ステップ36)。次にデータ暗号化部14及びデータ鍵暗号化部15は、それぞれ暗号化されたデータDT(EK)及び暗号化されたデータ鍵EK(DP)を通信制御部19を介してサーバ5へ送信する(ステップ37)。通信制御部27は、このデータ及びデータ鍵を受信し、データ及びデータ鍵アクセス部24を介してそれぞれデータ211及びデータ鍵212として両者を対応づけて記憶装置21に格納する(ステップ54)。

【0014】図3a及び図3bは、サーバ5に格納されたデータを参照するときの端末装置3、サーバ5及び鍵管理装置8の処理の流れを示すフローチャートである。端末装置3の入出力部12は、対象となるデータの名称、例えばファイル名を入力し、通信制御部19を介してサーバ5へデータ要求を送信する(ステップ41)。サーバ5の通信制御部27は、この要求を受信し(ステップ61)、ユーザの認証をした後、参照・登録権判定部25は、参照・登録権テーブル23を参照して要求されたデータの参照が妥当か否かを判定する(ステップ62)。要求が妥当であれば、データ鍵アクセス部24は、指定されたデータ211と対応するデータ鍵212とを送信する(ステップ63)。入出力部12は、このデータ211及びデータ鍵212を受信し(ステップ42)、個人鍵アクセス部16を介して公開個人鍵111を取り出し(ステップ43)、この公開個人鍵111及び受信したデータ鍵212を通信制御部19を介してサ

7

サーバ5へ送信する(ステップ44)。通信制御部27はこの公開個人鍵111及びデータ鍵212を受信し(ステップ64)、部門鍵アクセス部26は秘密部門鍵222を取り出して(ステップ65)、端末装置3から受け取った公開個人鍵111とデータ鍵212並びに取り出した秘密部門鍵222を通信制御部27を介して鍵管理装置8へ送信する(ステップ66)。鍵管理装置8の秘密部門鍵復号部73は、通信制御部75を介してこれらの情報を受信し(ステップ81)、マスタ鍵アクセス部72を介して秘密マスタ鍵712を取り出し(ステップ82)、秘密マスタ鍵712によって秘密部門鍵222を復号し(ステップ83)、復号された秘密部門鍵DSでデータ鍵212を復号する(ステップ84)。次にデータ鍵暗号化部74は、公開個人鍵111によって得られたデータ鍵EKを暗号化し(ステップ85)、通信制御部75を介してサーバ5へこのデータ鍵EK(PP)を送信する(ステップ86)。通信制御部27はこのデータ鍵を受信し(ステップ67)、端末装置3へ転送する(ステップ68)。端末装置3のデータ鍵復号部17は、通信制御部19を介してこのデータ鍵EK(PP)を受信し(ステップ45)、個人鍵アクセス部16を介して秘密個人鍵112を取り出し(ステップ46)、データ鍵EK(PP)を秘密個人鍵112によって復号する(ステップ47)。次にデータ復号部18は得られたデータ鍵EKによって先に受信したデータ211を復号し(ステップ48)、入出力部12が復号されたデータを出力装置に出力する(ステップ49)。

【0015】図4は、データ211、データ鍵212と機密区分との関連を説明する図である。機密区分は、レベル1、レベル2、・・・のように区分される。機密区分の各レベルは、後述するようにユーザのグループと関連付けられており、各ユーザグループは参照・登録権テーブル23に登録されているレベルの部門鍵しか利用できない。データ鍵によって暗号化されたデータ211は、機密区分とは独立である。公開部門鍵221及び秘密部門鍵222は、それぞれ機密区分のレベルに対応して設定されるので、公開部門鍵221によって暗号化され、秘密部門鍵222によって復号されるデータ鍵212は、機密区分のいずれかのレベルに対応して登録される。

【0016】図5は、データの参照又は登録に先立って行うユーザの認証処理の例を説明する図である。サーバ5は、各ユーザのユーザ名とパスワードとの対応テーブル、認証用公開鍵及び認証用秘密鍵を記憶装置に保持する。端末装置3は入力されたユーザ名(ユーザコード)をサーバ5へ送信する。サーバ5の図示しない認証処理部は、このテーブルを参照してユーザ名が登録してあれば、認証用公開鍵IPを端末装置3へ送信する。端末装置3は入力されたパスワードをこの認証用公開鍵で暗号化してサーバ5へ送る。サーバ5は、暗号化されたパス

8

ワードPWA(IP)を認証用秘密鍵ISで復号してパスワードPWAを得て、テーブル上のユーザ名Aに対応するパスワードPWAと照合する。パスワードが一致すれば、サーバ5は操作を許可するメッセージを端末装置3へ送信し、端末装置3はデータの参照又は登録の要求を送信する。なお認証用公開鍵及び認証用秘密鍵は適当な頻度で新しい鍵に変更されるものとする。

【0017】図6は、参照・登録権判定部25が行うデータの参照権及び登録権を判定する処理の具体例を説明する図である。ユーザの認証処理に使用されるユーザ名とパスワードの対応テーブルは、各ユーザごとにそのユーザの属するユーザグループの識別子を保持している。また参照・登録権テーブル23は、各グループごとにデータ参照を許可する機密区分のレベルとデータ登録を許可する機密区分のレベルとを設定する。データ登録権のあるユーザはそのデータを更新することもできる。例えばユーザ名Aのユーザは、ユーザグループG1に属するので、機密区分がレベル1のデータしか参照できない。また機密区分がレベル1のデータしか登録できない。またデータ鍵の機密区分を変更する場合には、ユーザは変更前のデータの参照権と変更後のデータの登録権を必要とする。例えば機密区分をレベル1からレベル2に変更する場合には、グループGpに属するユーザのようにレベル1のデータの参照権とレベル2のデータの登録権が必要である。図6の例において機密区分のレベルnは、他システムへデータを転送する権限を設定する。従って例えばグループGkに属するユーザのようにレベルnのデータについて登録権のあるユーザのみが他システムへデータを転送できる。

【0018】上記実施形態によれば、サーバ5に格納されるデータ鍵212は機密区分に対応して暗号化されるとともに参照・登録権テーブル23に従って参照・登録権のチェックを行うので、その機密区分をもったデータについて参照・登録権のあるユーザだけがそのデータを参照・登録できる。特に機密性の高いレベルのデータが機密性の低いレベルのデータに書き換えられることがないように参照・登録権テーブル23の機密区分のレベルを機密性の程度に応じて設定し、各ユーザグループに許可する機密区分のレベルを制限することによって、機密性の高いデータのセキュリティを強化できる。またユーザはいずれかのユーザグループに属するので、そのユーザグループに対して許可される機密区分をもったデータを共有することができる。データ鍵212は機密区分に対応しているが、データ211は機密区分から独立しているので、ネットワークを介してデータ211を伝送したりデータ211を復号することなくデータ鍵EK(DP)の機密区分を変更することが可能である。ステップ84でデータ鍵212が復号された後は、データ鍵EKは機密区分から独立となる。そしてステップ85で公開個人鍵によって暗号化されてネットワークを介して端末

装置 3 まで伝送されるので、ネットワーク伝送中のデータ鍵 EK の盗聴は実質的に無効である。またサーバ 5 の管理者は秘密マスタ鍵 2 2 2 を復号できず、従ってデータ鍵 2 1 2 を復号できず、実質的にデータ 2 1 1 にアクセスできない。さらに本発明は、オペレーティングシステムに依存せずアプリケーションプログラムのレベルで実現できるので、特定のハードウェアやオペレーティングシステムには依存しないアクセス制御が可能である。

【0019】図 7 は、本発明を適用するシステム形態の例を示す図である。システム A 及びシステム B は、それぞれ端末装置 3、3'、サーバ 5、5' 及び鍵管理装置 8、8' から構成され、システム A とシステム B は通信網を介して接続されている。

【0020】公開部門鍵 2 2 1 及び対となる秘密部門鍵 2 2 2 を機密区分ごとに設けておくことによってデータ鍵 2 1 2 が機密区分の役割を果たし、その機密区分のデータについてアクセス権をもつユーザグループの間でデータを共有できる。またデータ DT 1 (EK 1) に対応するデータ鍵 EK 1 (DP 1) の公開部門鍵 2 2 1 を DP 2 に変更する場合には、端末装置 3 から元のデータ鍵 2 1 2 と変更後の機密区分とをサーバ 5 へ送信し、サーバ 5 は秘密部門鍵 DS 1 (MP)、データ鍵 EK 1 (DP 1) 及び公開部門鍵 DP 2 を鍵管理装置 8 へ送信し、鍵管理装置 8 は秘密マスタ鍵 MS によって秘密部門鍵 DS 1 (MP) を復号し DS 1 を得る。次に DS 1 を用いてデータ鍵 EK 1 (DP 1) を復号し EK 1 とした後、新たな公開部門鍵 DP 2 によってデータ鍵 EK 1 を再度暗号化してデータ鍵 EK 1 (DP 2) を得る。これを受けたサーバ 5 は記憶装置 2 1 に格納されるデータ鍵 EK 1 (DP 1) をデータ鍵 EK 1 (DP 2) によって更新する。これによってデータ DT 1 (EK 1) を復号することなくデータの機密区分を変更できる。システム A からシステム B にデータを伝送する場合も同様にデータ鍵 EK 1 (DP 1) について上記と同様の手順を実行し他システム B の公開部門鍵 DP 1' によって再暗号化することによって安全に他システム B へデータを伝送することができる。

【0021】以上述べたように、データの参照と登録、データの機密区分の変更、他システムへデータ伝送する場合には必ずサーバ 5 が介入してユーザの認証に続いてデータ操作の権限をチェックするので、権限のない人間が不正にデータを取得したり勝手にデータを配布する操作を防止することができる。またサーバ 5 から端末装置 3 へ送信するデータ及びデータ鍵が盗聴されたとしても、データ鍵は公開部門鍵又は公開個人鍵によって暗号化されているので秘密部門鍵又は秘密個人鍵を知らなければ復号できず、従ってデータの機密性を確保できることが理解される。

【0022】なお上記実施形態では、鍵管理装置 8 をサーバ 5 から独立した装置として設けたが、サーバ 5 側の

記憶装置 2 1、記憶装置 2 2、データ及びデータ鍵アクセス部 2 4、参照・登録権判定部 2 5、部門鍵アクセス部 2 6 と鍵管理装置 8 の記憶装置 7 1、マスタ鍵アクセス部 7 2、秘密部門鍵復号部 7 3、データ鍵暗号化部 7 4 とが独立した関係に保たれるならば、鍵管理装置 8 の各処理部及びデータ部をサーバ内に設けてもよい。なおサーバ 5 の管理者に信頼を置くのであれば、マスタ鍵を設けず秘密部門鍵 DS を暗号化しないものとしてもよい。また上記実施形態では 1 つのサーバ 5 に対して 1 台の鍵管理装置 8 及び 1 つのマスタ鍵を設けたが、複数のサーバ 5 と鍵管理装置 8 の各々について複数のマスタ鍵を設けることも可能である。また複数のサーバ 5 に対して 1 台の鍵管理装置 8 を設けることも可能である。また本実施形態に示したユーザ認証方式はあくまで一つの例であり、ケルベロス認証等の他の個人認証技術を使うことが可能である。

#### 【0023】

【発明の効果】以上説明したように本発明によれば、暗号通信技術を用いてユーザグループの間で安全にデータを共有でき、しかも特別なハードウェアやオペレーティングシステムに依存しないアクセス制御を実現できる。

#### 【図面の簡単な説明】

【図 1】実施形態のアクセス制御システムの構成図である。

【図 2】実施形態のデータ登録時の端末装置 3 及びサーバ 5 の処理の流れを示すフローチャートである。

【図 3 a】実施形態のデータ参照時の端末装置 3 及びサーバ 5 の処理の流れを示すフローチャートである。

【図 3 b】実施形態のデータ参照時の鍵管理装置 8 の処理の流れを示すフローチャートである。

【図 4】データ、データ鍵及び機密区分の関連を説明する図である。

【図 5】ユーザ認証処理の例を説明する図である。

【図 6】実施形態のデータの参照権及び登録権を判定する処理を説明する図である。

【図 7】本発明を適用するシステム形態の例を示す図である。

【図 8】従来の暗号通信システムの構成を示す図である。

#### 【符号の説明】

3：端末装置、5：サーバ、8：鍵管理装置、13：データ鍵生成部、14：データ暗号化部、15：データ鍵暗号化部、17：データ鍵復号部、18：データ復号部、23：参照・登録権テーブル、25：参照・登録権判定部、73：秘密部門鍵復号部、74：データ鍵暗号化部、111：公開個人鍵、112：秘密個人鍵、211：データ、212：データ鍵、221：公開部門鍵、222：秘密部門鍵、711：公開マスタ鍵、712：秘密マスタ鍵



【図 1】

【図 3 b】

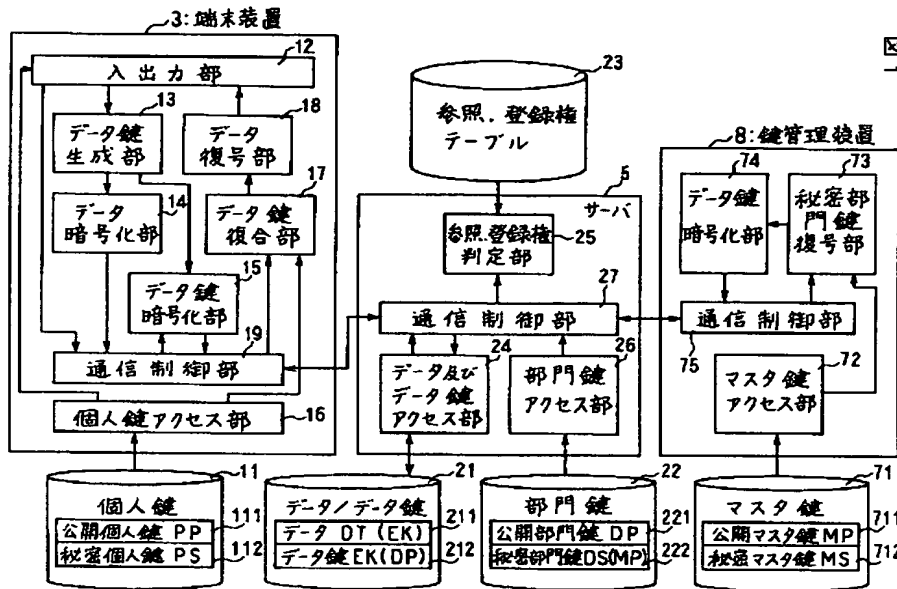
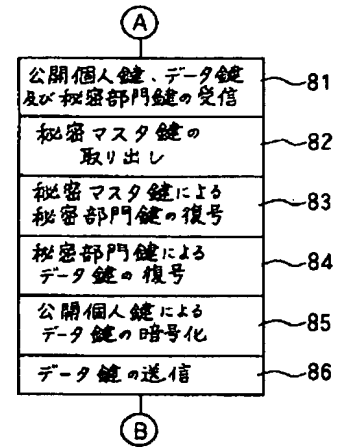


図 3b

鍵管理装置 8

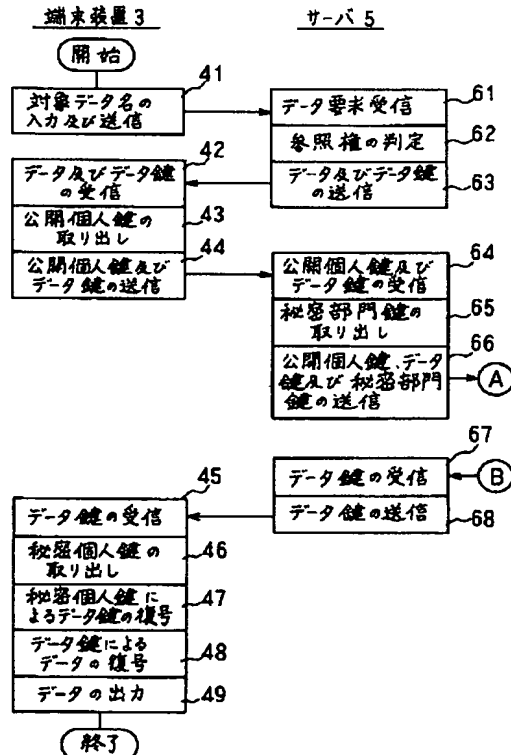
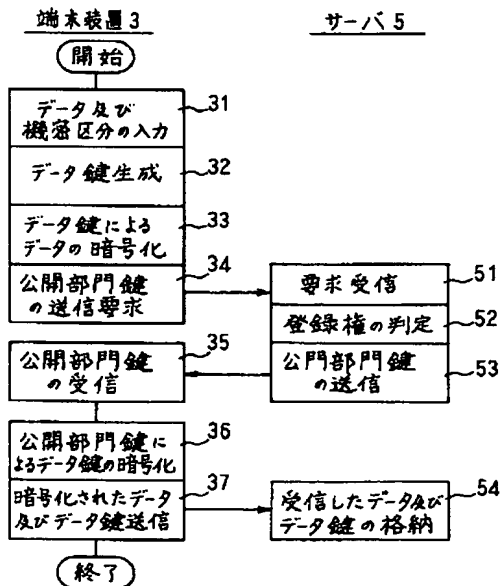


【図 2】

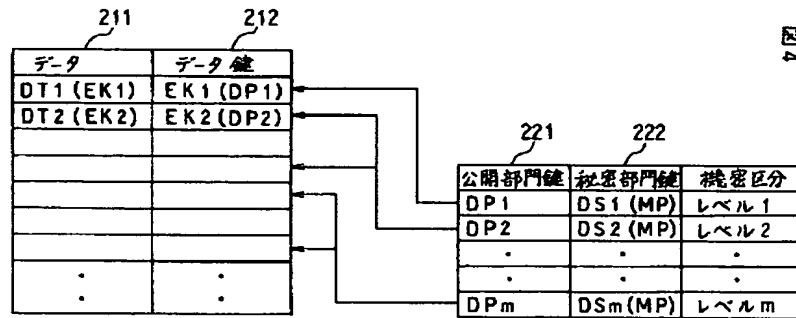
【図 3 a】

図 2

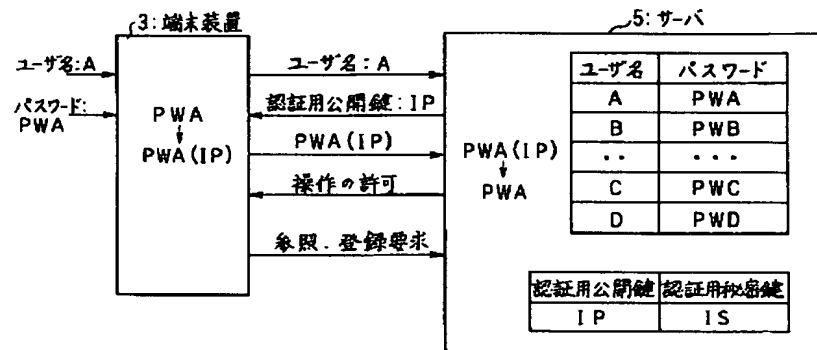
図 3a



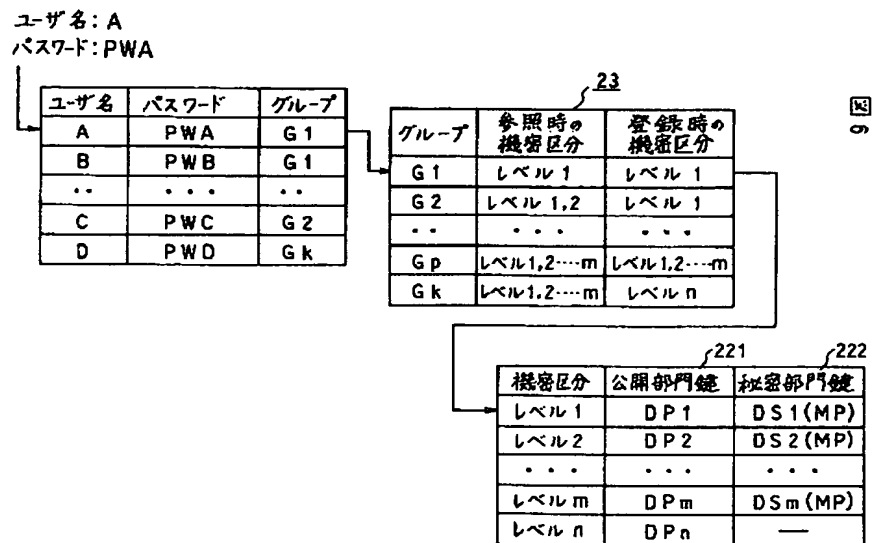
【図 4】



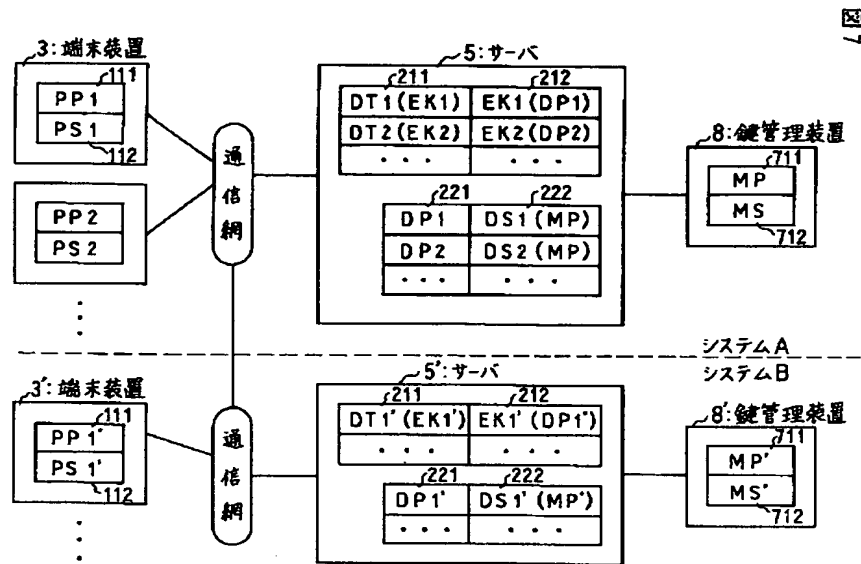
【図 5】



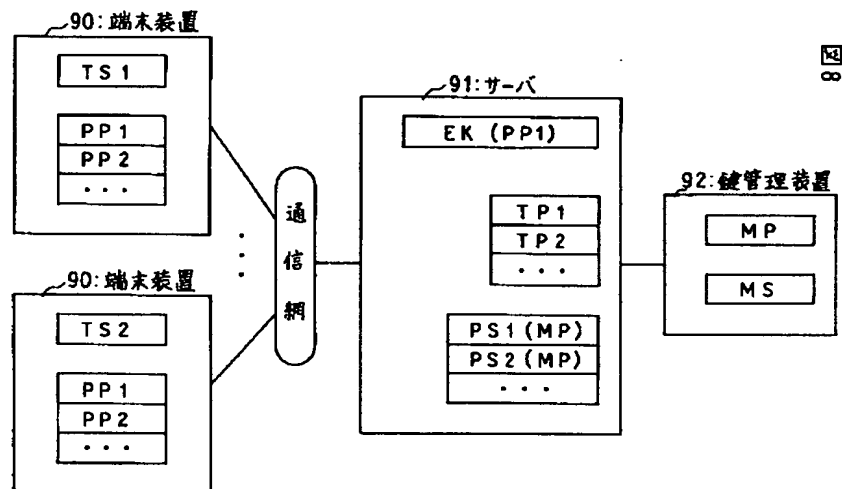
【図 6】



【図7】



【図8】



フロントページの続き

(72) 発明者 宝木 和夫  
 神奈川県川崎市麻生区王禅寺1099番地 株  
 式会社日立製作所システム開発研究所内

(72) 発明者 柴原 節男  
 東京都江東区新砂一丁目6番27号 株式会  
 社日立製作所公共情報事業部内